PRIVACY POLICY

CONVRS Communication Training Platform

Version 1.2 | Effective Date: April 2026 | Last Updated: April 2026
Click-Through on Platform | Incorporated in Master Services Agreement
Smarter Reality, LLC | Round Rock, Texas | convrsplatform.com | frank@smarterreality.io

Smarter Reality, LLC ("We," "Us," or "Our"), located at Round Rock, Texas, USA, is committed to protecting the privacy and security of data collected through CONVRS (the "Platform"), our subscription-based VR communication and de-escalation training platform designed exclusively for professional law enforcement and training organizations.

This Privacy Policy describes how We collect, use, disclose, store, and protect information in connection with the Platform. By accessing or using the Platform, or by your Agency executing a Master Services Agreement or Order Form, you acknowledge that you have read this Privacy Policy and agree to its terms.

1. Who This Policy Applies To

This Policy applies to: (a) the law enforcement agency or training organization ("Agency") that has executed a Master Services Agreement with Us; (b) individual officers, trainers, and authorized administrators who access the Platform under the Agency's Department License; and (c) visitors to convrsplatform.com.

The Platform is designed exclusively for professional law enforcement use by adults (18+). It is not directed at individuals under 18, and We do not knowingly collect personal data from minors.

2. Information We Collect

2.1 Account and Agency Information

Agency name, contact details (administrator email, billing information), Department Size Tier, licensed seat count, payment-related data (processed securely; We do not store full credit card numbers), and tax-exemption status.

2.2 Training and Performance Data

Anonymized or pseudonymized metrics from training sessions, including scenario completion rates, decision paths, de-escalation outcome scores, feedback analytics, and compliance data (e.g., training hours for POST or equivalent reporting). Such data is associated with officer identifiers configured by Agency (e.g., badge number or username), not with personally identifiable information such as legal name or Social Security Number, unless Agency specifically configures the Platform to use such identifiers.

2.3 CONVRS Curriculum Usage Data

Data related to Agency's use of the CONVRS Curriculum, including trainer session logs, briefing and debrief records, and curriculum progression data, where tracked by the Platform.

2.4 Sensor and Physiological Data (Optional)

If Agency enables wearable sensor integration, anonymized stress indicators (e.g., heart rate variability) may be collected and used solely for real-time training feedback and aggregated analytics. We do not collect or store identifiable biometric templates, facial recognition data, or voiceprints for identification purposes.

2.5 Technical Data

IP address, device type, Meta Quest 3 headset model and firmware version, system logs, and error reports, collected for troubleshooting, security, and Platform improvement purposes.

2.6 Agency Content

Any custom scenarios, supplemental materials, or other content created or uploaded by Agency is treated as Agency's confidential information per the MSA. We process such content only as directed by Agency and solely for the purpose of providing the Platform.

3. How We Use Information

We use information solely for purposes related to providing and improving the Platform:

- Providing, maintaining, and improving CONVRS and the CONVRS Curriculum.
- Generating anonymized analytics and compliance reports (e.g., POST training hours, de-escalation outcome metrics).
- Supporting Agencies with troubleshooting, account management, and technical assistance.
- Processing payments and managing subscriptions (via accepted payment methods including PO, check, and organizational credit card).
- Complying with applicable legal obligations (e.g., audits, export controls, lawful legal process).
- Developing aggregated product insights to enhance evidence-based training content. We use only anonymized, aggregated data for this purpose and do not identify individual officers.

We do not use data for advertising, marketing to individuals, or for any purpose unrelated to the Platform.

4. Sharing and Disclosure

We do not sell Personal Data. We share information only as necessary:

- With Sub-Processors (e.g., cloud hosting, AI model providers, analytics tools) under strict contractual data protection obligations as described in the Data Processing Agreement.
- To comply with applicable laws, valid legal process, or government audits. We will endeavor to notify Agency of any legal demands for Agency's data unless prohibited by law.
- In connection with a merger, acquisition, or asset sale, with advance notice to affected Agencies as required by applicable law.
- With Agency's express written consent for specific integrations or authorized sharing.

5. Data Anonymization and Aggregation

Most training performance data is anonymized or aggregated to protect individual officer privacy while enabling product improvements and compliance reporting. We do not re-identify anonymized data.

6. Data Security

We implement commercially reasonable administrative, technical, and physical safeguards appropriate to the law enforcement technology context, including: encryption in transit (TLS 1.2+) and at rest (AES-256 or equivalent); role-based access controls; regular security assessments; and incident response procedures. Agencies with CJIS or other government security requirements may request Our full security documentation.

7. Data Retention

We retain data for as long as necessary to provide the Platform, comply with legal obligations, resolve disputes, and enforce agreements. Upon termination, Agency may request deletion of its Personal Data per the Data Processing Agreement. Anonymized and aggregated data may be retained indefinitely for Platform improvement. Backup copies may be retained for up to ninety (90) days after a deletion request is fulfilled.

8. Agency Rights and Controls

Agencies act as data controllers for Personal Data relating to their officers. We assist Agencies in:

- Responding to individual officer requests to access, correct, or delete training records (routed through Agency administrators).
- Opting out of optional analytics features through Platform settings.
- Obtaining a data export upon request, subject to technical feasibility and reasonable advance notice.

For direct privacy inquiries: frank@smarterreality.io

9. CJIS Compliance

For Agencies subject to FBI CJIS Security Policy requirements, We will cooperate to support compliance. Agencies are responsible for ensuring their use of the Platform aligns with applicable CJIS requirements. Contact Us for CJIS compliance documentation. We will execute a CJIS Security Addendum upon request if required.

10. Changes to This Policy

We may update this Privacy Policy from time to time. Material changes will be communicated via email to Agency's administrator or via in-Platform notification at least fourteen (14) days before the effective date. Continued use of the Platform after the effective date constitutes acceptance of the updated Policy.

11. Contact Us

Questions, concerns, or privacy requests? Contact:

Smarter Reality, LLC — Privacy Officer | frank@smarterreality.io | convrsplatform.com | Round Rock, Texas, USA

This Privacy Policy is presented as a click-through acceptance on the Platform and is also incorporated by reference into the Master Services Agreement as Appendix C.